# Quantum Information Science

*R. J. Hughes, W. T. Buttler,*
*M. H. Holzscheiter, P. G. Kwiat,*
*S. K. Lamoreaux, G. L. Morgan,*
*C. G. Peterson, C. Simmons,*
*A. G. White (P-23),*
*G. G. Luther (P-22),*
*M. Schauer (P-24),*
*M. S. Gulley, V. Sandberg,*
*D. Tupa (P-25),*
*A. G. Petschek (P-DO),*
*R. Laflamme, W. H. Zurek (T-6),*
*D. F. V. James (T-4),*
*J. E. Nordholt (NIS-1),*
*J. M. Ettinger (NIS-8),*
*M. S. Neergaard (NIS-9),*
*E. Knill (CIC-3)*

## Introduction

The representation of information by classical physical quantities such as the voltage levels in a microprocessor is familiar to everyone. But over the past decade, quantum information science has been developed to describe binary information in the form of two-state quantum systems, such as photon polarization states. (A single bit of information in this form has come to be known as a "qubit.") Remarkable new capabilities in the world of information security have been predicted that make use of quantum-mechanical superpositions of information, a concept that has no counterpart in conventional information science. For example, quantum cryptography allows two parties to communicate securely even in the presence of hostile monitoring by a third party. A quantum computer would make use of logical operations between many qubits and would be able to perform many operations in parallel. Certain classically intractable problems, such as factoring large integers, could be solved efficiently on a quantum computer. We have experimental projects underway in quantum cryptography, quantum computation, and interaction-free measurement, which also takes advantage of quantum properties.

## Quantum Cryptography

One of the main goals of cryptography is for two parties ("Alice" and "Bob") to render their (binary) communications unintelligible to a third party ("Eve"). This can be accomplished if Alice and Bob both possess a secret random-bit sequence, known as a cryptographic key. For example, in "one-time pad" encryption Alice adds the key to the original message, known as plaintext, and communicates the sum (ciphertext) to Bob. He is able to recover the plaintext by subtracting his key from the ciphertext, but Eve, who is assumed to have monitored the transmitted ciphertext, is unable to discern the underlying plaintext through the randomization introduced with Alice's key. So, although key material conveys no useful information itself, it is a very valuable commodity, and methods for Alice and Bob to generate key material securely are correspondingly important.

Using quantum cryptography, or, more accurately, quantum key distribution (QKD), Alice and Bob can create shared cryptographic key material whose security is assured by the laws of quantum mechanics. They first independently generate secret random-number sequences, which then undergo a bit-wise comparison that requires the preparation, transmission, and measurement of a single photon for each bit. Alice's photon-state preparations and Bob's measurements are determined by their bit values and are chosen from sets of nonorthogonal possibilities, such as linear and circular polarization. This comparison algorithm, which may be publicly known, ensures that Bob detects a photon (with some quantum-mechanically determined probability) only if he has the same bit value as Alice. They retain only the detected bits from their initial sequences. These subsets are the raw key material from which a pure key is distilled using classical error-detection

techniques. Eve can neither "tap" the key transmissions (owing to the indivisibility of a photon) nor copy them (owing to the quantum "no-cloning" theorem). Furthermore, the nonorthogonal nature of the quantum states ensures that if Eve makes her own measurements, she will be detected through the elevated error rate arising from the irreversible "collapse of the wave function" that she introduces.

QKD offers many security and ease-of-use advantages over existing key-distribution methods. Traditional key distribution using trusted couriers requires cumbersome security procedures for preparing, transporting, and handling the key before any communications can take place and may even be impractical (e.g., re-keying a satellite). In contrast, quantum keys do not even exist before the QKD transmissions are made, and a key can be generated at message-transmission time. Public-key cryptography also avoids many of the difficulties of key distribution by courier but provides only the conditional security of intractable mathematical problems, such as integer factorization. Accurate assessment of an adversary's computing power over the useful lifetime of encrypted information, which may be measured in years or even decades, is notoriously difficult: unanticipated advances in fields such as quantum computation could render public-key methods not just insecure in the future but also retroactively vulnerable. QKD could be used for real-time key generation in cryptographic applications where this long-term risk is unacceptable.

The physical systems that can support QKD transmissions determine the potential uses of quantum cryptography. We have demonstrated that QKD is possible over multikilometer optical-fiber paths: the necessary quantum coherence of the QKD transmissions persists even outside the controlled environment of a physics laboratory. At the infrared wavelengths required, germanium or indium-gallium arsenide avalanche photodiodes can be persuaded to detect single photons but at the penalty of a high noise and, hence, a high error rate. Removing these errors reduces the amount of key material and limits transmission distances to 100 km or so. (Optical amplifiers cannot be used to extend this range because they cannot replicate the nonorthogonal quantum states used in QKD.)

In our experiment we demonstrated quantum cryptography over 24 km of optical fiber that had been installed for network applications between two LANL technical areas. We have recently increased the propagation distance to 48 km; Fig. II-13 shows the system that was used in this demonstration. Our system incorporates an encryption/decryption feature that allows us to use the quantum-key material to encrypt short text messages at the sending computer and decrypt them at the receiving computer. This experiment shows that QKD could be used to generate cryptographic keys over "open" optical-fiber links between secure "islands," such as between different government agencies in the Washington, D.C., area.

In a separate experiment we are developing QKD for "free-space," line-of-sight communications, such as surface-to-aircraft. This technology could also possibly be used for the re-keying of satellites in low-earth orbits. So far, we have achieved low-error-rate transmissions over 205 m within our laboratory, but we will extend this distance to several kilometers in the near future. These new experiments will take place outdoors and will allow us to assess the daylight background and atmospheric optics issues that will impact the key rate and error rate. Quantum cryptography is likely to be the first practical application of the foundations of quantum mechanics, which illustrates the often unexpected value of basic research.

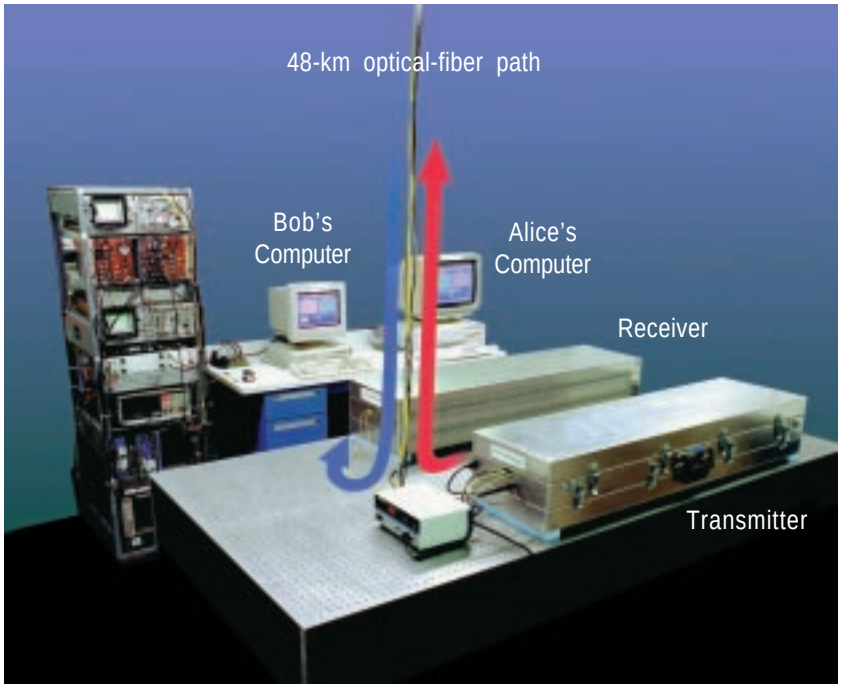


***Fig. II-13. The 48-km quantum-cryptography system.***

## Quantum Computation

With two or more qubits it becomes possible to consider quantum logical-gate operations in which a controlled interaction between qubits produces a coherent change in the state of one qubit that is contingent upon the state of another. These gate operations are the building blocks of a quantum computer (QC), which in principle is a very much more powerful device than any classical computer because the superposition principle allows an extraordinarily large number of computations to be performed simultaneously. In 1994 it was shown that this "quantum parallelism" could be used to efficiently find the prime factors of composite integers. Integer factorization and related problems that are computationally intractable with conventional computers are the basis for the security of modern public-key cryptosystems. However, a quantum computer running at desktop PC speeds could break the keys of these cryptosystems in only seconds (as opposed to the months or years required with conventional computers). This single result has turned quantum computation from a strictly academic exercise into a subject whose practical feasibility must be urgently determined.

The architecture of a quantum computer is conceptually very similar to a conventional computer: multiqubit, or "multibit," registers are used to input data; the contents of the registers undergo logical-gate operations to effect the desired computation under the control of an algorithm; and, finally, a result must be read out as the contents of a register. The principal obstacles to constructing a practical quantum computer are (1) the difficulty of engineering the quantum states required; (2) the phenomenon of "decoherence," which is the propensity for these quantum states to lose their coherence properties through interactions with the environment; and (3) the quantum measurements required to read out the result of a quantum computation. The first proposals for practical quantum-computation hardware, based on various exotic technologies, suffered from one or more of these problems.

In 1994 it was proposed that the basic logical-gate operations of quantum computation could be experimentally implemented with laser manipulations of cold, trapped ions (Fig. II-14): a qubit would comprise the ground (S) state (representing binary 0) and a suitably chosen metastable excited (D) state (to represent binary 1) of an ion isolated from the environment by the electromagnetic fields of a linear radio-frequency quadrupole (RFQ) ion trap.

The principal components of this technology are already well developed for frequency-standard and high-precision spectroscopy work. Existing experimental data suggest that adequate coherence times are achievable, and a read-out method based on so-called "quantum jumps" has already been demonstrated with single trapped ions. We are developing an ion-trap quantum-computer experiment using calcium ions, with the ultimate objective of performing multiple gate operations (and possibly small computations) on a register of several qubits in order to determine the potential and physical limitations of this technology.

The heart of our experiment is a linear RFQ ion trap with cylindrical geometry in which strong radial confinement is provided by radio-frequency potentials applied to four "rod" electrodes and axial confinement is produced by a harmonic electrostatic potential applied by two "end caps." After laser cooling on their 397-nm S-P transition, several calcium ions will become localized along the ion trap's axis because their recoil energy (from photon emission) is less than the spacing of the ions' quantum vibrational energy levels in the axial confining potential. Although localized to distances much smaller than the wavelength of the cooling radiation, the ions nevertheless undergo small amplitude oscillations, and the lowest frequency mode is the axial center of mass (CM) motion in which all the ions oscillate in phase along the trap axis. The frequency of this mode, whose quantum states will provide a computational "bus," is set by the axial potential. The inter-ion spacing is determined by the equilibrium between this axial potential, which tends to push the ions together, and the ions' mutual Coulomb repulsion. For example, with a 200-kHz axial CM frequency, the inter-ion spacing is on the order of 30 μm.

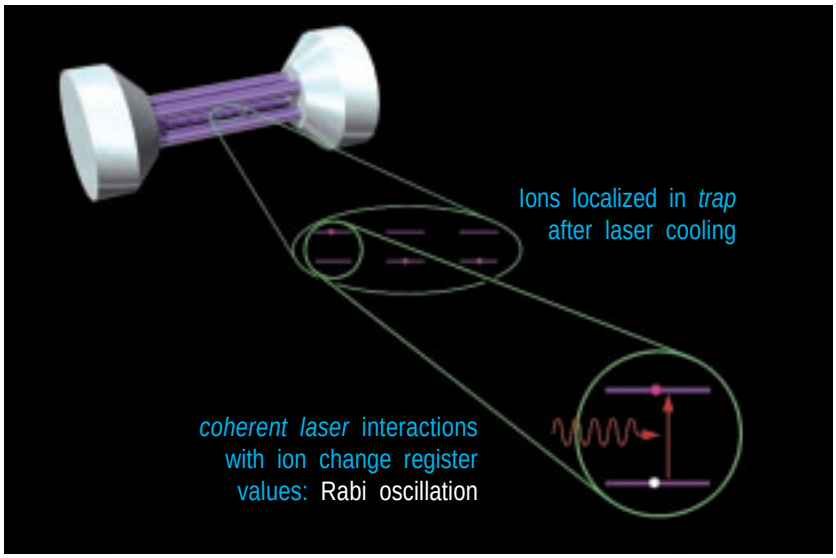


***Fig. II-14. A schematic representation of the ion traps and logical gates created by laser-manipulated ions in quantum computation.***

Because of its long radiative lifetime (~1 s), the S-D transition has such a narrow width that it develops upper and lower sidebands separated from the central frequency by the CM frequency. With a laser that has a suitably narrow linewidth and is tuned to the lower sideband, an additional stage of laser cooling is used to prepare the "bus" qubit (CM vibrational mode) in its lowest quantum state ("sideband cooling"). On completion of this stage, the QC is prepared with all qubits in the $|0\rangle$ state, ready for quantum computation.

The narrow-linewidth laser tuned to the S-D transition is the essential tool for changing the contents of the quantum register of ions and performing quantum logical-gate operations. By directing this laser at an individual ion for a prescribed time, we will be able to coherently change the value of the qubit that the ion represents through the phenomenon of Rabi oscillations. An arbitrary logical operation can be constructed from a small set of elementary quantum gates, such as the so-called "controlled-NOT" operation, in which the state of one qubit is flipped if a second qubit is in the "1" state but left unchanged if the second qubit is in the "0" state. This gate operation can be effected with three laser operations, using quantum states of the ion's CM motion as a computational bus to convey quantum information from one ion to the other. The result of the quantum computation can be read out by turning on the S-P laser. An ion in the "0" state will fluoresce, whereas an ion in the "1" state will remain dark. So, by observing which ions fluoresce and which are dark, a value can be obtained. We have recently succeeded in trapping calcium ions in our ion trap and imaging them with a charge-coupled device (CCD) camera. This is the first step toward creation of a quantum register.

We have also studied the intrinsic computational potential of ion-trap QCs. By taking into account the relevant decoherence mechanisms, we have found that on the order of one million gate operations could be performed on registers of 50 or so ions. This is a tremendous amount of quantum computation relative to the current state of the art: one logic operation on two qubits. Furthermore, because a QC can create an arbitrary quantum state using quantum logic operations, this computational capacity opens up a wide variety of quantum-mechanics experiments in domains that are today computationally inaccessible. We expect therefore that ion-trap QCs will allow us to explore quantum computation and the foundations of quantum mechanics.

## Interaction-Free Measurement

Another area of great interest in the study of the role of quantum mechanics in information is that of "interaction-free measurements," in which the existence of nontransmitting objects (absorbers or scatterers) can be ascertained with arbitrarily small absorption/scattering taking place. In the simplest scheme, an interferometer is tuned for complete destructive interference for one of the output ports. The presence of an object in one of the arms removes the possibility of interference, so that a detector in the "dark" output port now has a chance of detecting an incident photon, which was not possible in the absence of the object. By varying the reflectivity of the inteferometer beam splitters, up to 50% of the measurements can be made interaction-free, as has been demonstrated in our lab.

More amazing, the fraction of interaction-free measurements can actually be made arbitrarily close to 1 by using a repeated interogation scheme—an application of the "Quantum Zeno" effect. In this case, there is an arbitarily small chance that any photons are absorbed by the object, and yet one gains definite information about its presence because the object inhibits an otherwise coherent evolution of the interrogating photon. For example, using simple optical elements, the polarization state of the photon can be made to rotate in small, equal steps from horizontal to vertical. However, the presence of an object that absorbs only the vertical component of the polarization at each stage will inhibit this rotation by collapsing the photon's wave function at each step back into the initial horizontal polarization. The total probability that the photon is ever actually absorbed can be made arbitrarily small by using many steps. Thus, without the object, the final state of polarization is vertical, but with the object present, the polarization becomes "trapped" in the horizontal. Paradoxically, it is the very presence of the absorbing object that alters the quantum state of the interrogating particle, ensuring that it is only rarely absorbed.

At LANL (in collaboration with researchers from the University of Innsbruck), we have achieved measurements that are up to 85% interaction free, which is the first demonstration to break the 50% limit. Efficiencies in excess of 95% are now being sought using a fast switching system. Also, we have begun investigating the practical implementation of interaction-free imaging, in which the techniques would be used to take a pixellated image of an object, again with the goal of negligible absorption or scattering. To date a resolution of less than 10 μm has been achieved in a simple, one-dimensional system looking at objects such as thin wires, optical fibers, and hairs. Finally, one of the most exciting prospects is the ability to couple to a quantum object, such as a single atom or ion, which can be in a superposition state. Using the techniques of interaction-free measurements, the quantum state can be transferred to the interrogating light, allowing the production of macroscopic entangled states of light and Schrödinger-cat states.

Please see the tutorial at http://p23.lanl.gov/Quantum/kwiat/ifm-folder/ifmtext.html for more information.